Regular languages and minimal saturated automata.

Abstract: A saturated automaton relative to a regular language R is a non-deterministic automaton accepting R, and which contains homomorphic images of all automata accepting R.

In this paper we construct a (unique) minimal saturated automaton for a given regular language R and prove some basic properties. In particular, we show that the states in this automaton may be given a lattice structure, and that the states in the minimal deterministic automaton relative to R naturally gives a generator set for this lattice.

And we describe how the homomorphisms from an arbitrary automaton accepting R into the minimal saturated automaton must behave. This is useful if one is interested in finding a state minimal non-deterministic automaton accepting R. It is also useful in giving lower bounds on the "star height" of R. The applications to the star height problem will not be treated here. (See [6])

1. Introduction

One of the main unsolved problems in the theory of regular events is the star height problem. The star height of a regular exprission is defined as the height (or depth) of the nesting of the $*$ operator. The start height of a regular event is defined as the minimum of the star heights of expressions denoting R.

The problem is how to determine in some explicit way the star height of an event R. The difficulty is that there are infinitely many regular expressions denoting one event R, or equivalently, there are infinitely many nondeterministic automata (NDA's) accepting R; see Eggan [3].

In this paper we single out a special automaton $\mathcal{A}$ which is "universal" relative to R, in the sense that $\mathcal{A}$ contains homomorphic images of all the infinitely many NDA's for R. Such a "universal element" should preferably be small.

We call an automaton $\mathcal{A}$ saturated relative to R if it satisfies the requirements

1) $\mathcal{A}$ accepts R;
2) for all NDA's $\mathcal{A}'$ accepting R there exists a homomorphism from $\mathcal{A}'$ to $\mathcal{A}$.

Our notion of homomorphism is given in definition 3.2. We are interested in homomorphisms that preserve paths and words, so if V' is an accepting path for w in $\mathcal{A}'$, we want the homomorphism ϕ: $\mathcal{A}' \to \mathcal{A}$ to induce an accepting path $V = \phi(V')$ for w in $\mathcal{A}$. This strengthens the requirements in McNaughton [7], but we find ours more ntural, one advantage being that a regular expression E' corresponding to $\mathcal{A}'$ will be transformed to a regular expression E corresponding to the image $\phi(\mathcal{A}')$ in $\mathcal{A}$.

We construct in this paper a minimal (unique) saturated automaton for any event R, denoted Sat(R). It is our hope to use this automaton to characterize the star height of R: for some results in this direction see [6]. But it is also our belief that the notion of saturated automata is of independent interest.

Part I of this paper gives an effective construction of Sat(R), and we point out the relationship with the automaton $\mathcal{A}_k(R)$ introduced by Cohen and Brzozowiski [2]. The $\mathcal{A}_k(R)$ automata are in substance saturated (see ex.4.1 with remark), but they are not <u>minimal</u> saturated automata.

The states of Sat(R) are the (finitely many) maximal pairs K_R. Following Kameda and Weiner [5] we introcue the reduced automaton matrix (RAM) which substansially simplifies the computation of maximal pairs. We also study the relationship of Sat(R) with Det(R), the minimal deterministic automaton accepting R, in some cases they are almost the same, but in other cases Sat(R) is much bigger than Det(R). We conclude part I with some examples and computations.

In part II we study some general properties of Sat(R). The states K_R can be ordered by a relation $<$ such that it becomes a lattice. In general this lattice is neither distrubutive nor modular. However, in section 9 we show that FD(n), the free distributive lattice with n generators, can be realized as $(K_{R(n)}, <)$ for some suitable events R(n).

We are also interested i generatorsets for $(K_R,<)$. Though the states K_R may be computed using RAM as we do in part I, having a generator set for $(K_R,<)$ would be useful. We study sufficient conditions for $A \subseteq K_R$ to generate K_R. We also show that Det(R) naturally is a subautomaton of Sat(R), and that the states in Det(R) is a generator set. (The same is true for BDet(R), the minimal backward determistic automaton for R)

In [5] the problem was to give an efficient algorithm for finding one minimal nondetermistic automaton with respect to R. There is no uniqueness about such an automaton, but since Sat(R) is saturated, it is clear that all minimal NDA's relative to R can be found as subautomata of Sat(R).

One algorithm for finding one (or all) minimal NDA's for R is the following:

a) Construct Sat(R).

b) For all subautomata $\mathcal{A}'$ of Sat(R),
   (starting with the smallest ones)
   check if $\mathcal{A}'$ accepts R:
   if "yes" $\mathcal{A}'$ is minimal, stop;
   if "no" continue with the next subautomaton.

In the algorithm of Kameda and Weiner [5] one does not construct Sat(R), but is only concerned with the small subautomata, (i.e. in essence step b).

Some shortcuts are possible in this algorithm, we are interested in the core of Sat(R), which is all the states and transitions in Sat(R) which are "absolutely necessary". Core(R) may be defined as the maximal part $\mathcal{C}$ of Sat(R) satisfying:

(*) if $\mathcal{C}' \subseteq \mathrm{Sat}(R)$ accepts R then $\mathcal{C} \subseteq \mathcal{C}'$

It is interesting to note that Core(R) is equal to the intersection of Det(R) and BDet(R) (in Sat(R)).

2 Preliminaries

We assume that the reader is familiar with the basic properties of regular expressions and finite (deterministic and nondeterministic) automata (DA's and NDA's).

In particular, we assume that the reader known how to construct, from an NDA $\mathcal{A}'$ for R, and equivalent NDA $\mathcal{A}$ without e-transitions, and further to construct $\mathcal{D}(\mathcal{A})$, the deterministic automaton equivalent to $\mathcal{A}$, by the subset construction; see sections 2.1 - 2.5 in Hopcroft and Ullman [4].

We shall also frequently use the minimization algorithm which reduces a DA $\mathcal{A}$ to the unique minimal DA called Det(R); see section 3.4 in [4].

Since we several places in this paper use definitions from [5], we have adopted their notation, thus deviating occasionally from Hopcroft and Ullman.

The basic notations.

An automaton (NDA) is a tuple

$\mathcal{A} = (Q, \Sigma, M, S_0, F)$

Σ is the (finite) input alphabet,

Q is the finitely many states,

S_0, $F \subseteq Q$ are the initial and final states,

$M \subseteq Q \times (\Sigma \cup \{e\}) \times Q$ is the <u>transition relation.</u>

If $\mathcal{A}$ is deterministic, we will write $\delta(q,a) = q'$ instead of $(q,a,q') \in M$. δ is extended in the usual way to a function $\delta: Q \times \Sigma^* \to Q$. We will also regard M as functions

$$M: Q \times \Sigma^* \to 2^Q,\quad M: 2^Q \times \Sigma^* \to 2^Q \quad \text{and} \quad M: 2^Q \times 2^{\Sigma^*} \to 2^Q$$

(extended in the usual way).

<u>$T(\mathcal{A})$</u> $= \{w \in \Sigma^* \mid M(S_0,w) \cap F \neq \emptyset\}$ is the regular event <u>accepted</u> by $\mathcal{A}$. We use the following abbreviation: $T(\mathcal{A},q,q') = T((Q,\Sigma,M,\{q\},\{q'\}))$

Further let $Pr^{\mathcal{A}}(q) = T(\mathcal{A}, S_0, q)$ be the <u>preceding event</u> and let $Sc^{\mathcal{A}}(q) = T(\mathcal{A},q,F)$ be the <u>succeding event.</u>

We say that q is a <u>dead state</u> iff $Sc(q) = \emptyset$, and that q is an <u>inaccesible state</u> iff $Pr(q) = \emptyset$. Such states are useless, and can be omitted:

$\mathcal{A}^-$ is the automaton $\mathcal{A}$ after removal of the useless states and the corresponding transitions.

We also need the following notions of <u>subautomata</u>:

$\mathcal{A} \restriction Q$ is $\mathcal{A}$ restricted to the states $Q' \subseteq Q$.

$\mathcal{A} - (q,a,q')$ is $\mathcal{A}$ without the transition (q,a,q').

We write <u>$Det(R)$</u> for the <u>minimal deterministic automaton</u> with respect to R obtained either by the Myhill-Nerode theorem, or by the usual minimization algorithm.

The dual of $\mathcal{A}$, $\overleftarrow{\mathcal{A}} = (Q, \Sigma, \overleftarrow{M}, F, S_0)$ is the automaton obtained by turning all arrows and interchange initial and final states. $\overleftarrow{\mathcal{A}}$ will accept the dual (transpose) event R^T. Like Det(R) we have also <u>BDet(R)</u>, the minimal <u>backward deterministic automaton</u> (BDA) and $(\mathrm{BDet}(R))^{\leftarrow} = \mathrm{Det}(R^T)$.

The notation in connection with Det(R) and BDet(R).

We define $u \overset{D}{\sim} v \pmod R$ iff $\forall w \in \Sigma^*(uw \in R \Leftrightarrow vw \in R)$ and

$u \overset{B}{\sim} v \pmod R$ iff $\forall w \in \Sigma^*(wu \in R \Leftrightarrow wu \in R)$

(These are the equivalence relations used in the Myhill-Nerode theorem.)

Further define $p \sim p' \pmod{\mathcal{A}}$ iff $Sc^{\mathcal{A}}(p) = Sc^{\mathcal{A}}(p')$. (This is the equivalence relation used in the minimization algorithm.)

Define $w\backslash R = \{u \in \Sigma^* \mid wu \in R\}$ and $R/v = \{u \in \Sigma^* \mid uv \in R\}$

We write $\mathrm{Det}(R) = (\hat{P}, \Sigma, \delta_D, p_e, F_D)$ and

$\mathrm{BDet}(R) = (\hat{Q}, \Sigma, \overleftarrow{\delta}_B, S_B, q_e)$

where we distinguish between the following two cases:

1) if these automata are constructed following the Myhill-Nerode theorem:

$\hat{P} = \{p_{[w]} \mid [w]$ is an equivalence class of $\overset{D}{\sim}\}$

$\hat{Q} = \{q_{\langle v\rangle} \mid \langle v\rangle$ is an equivalence class of $\overset{B}{\sim}\}$

$\delta_D(p_{[w]}, a) = p_{[wa]}$ $\quad \overleftarrow{\delta}_B(q_{\langle v\rangle}, a) = q_{\langle av\rangle}$

$p_e = p_{[e]}$ $\quad q_e = q_{\langle e\rangle}$

$F_D = \{p_{[w]} \mid w \in R\}$ $\quad S_B = \{q_{\langle v\rangle} \mid \overleftarrow{v} \in R\}$

This gives: $Pr^{\mathrm{Det}(R)}(p_{[w]}) = [w]$ $\quad Sc^{\mathrm{BDet}(R)}(q_{\langle v\rangle}) = \langle v\rangle$

$Sc^{\mathrm{Det}(R)}(p_{[w]}) = w\backslash R$ $\quad Pr^{\mathrm{BDet}(R)}(q_{\langle v\rangle}) = R/v$

2) If they are constructed using the minimization algorithm: Given a DA $\mathcal{A} = (P,\Sigma,M',p_0,F)$. Then $Det(R) \approx \mathcal{A}^\wedge = (\hat{P},\Sigma,\hat{M}',[p_0],\hat{F})$ where $\hat{P} = \{[p] | p \in P\}$ (i.e. we identity equivalent states). Similar notations are used for BDet(R).

If $\mathcal{A}$ is a NDA accepting R, then $Det(R) \approx \mathcal{D}(\mathcal{A})^\wedge$ and $BDet(R)^{\leftarrow} \approx \mathcal{D}(\mathcal{A}^{\leftarrow})^\wedge$.

We will also use $\hat{P}$ $(\hat{Q})$ for the states in $Det^-(R)(BDet^-(R))$

A <u>path</u> in $\mathcal{A}$ consists of (0 or more) transitions, and will be written $V = (q^0,a^1,q^1,\ldots,a^k,q^k)$ $k \geq 0$ $a^i \in \Sigma \cup \{e\}$ where $(q^i,a,q^{i+1}) \in M$ or $(q^i,a,q^{i+1}) = (q,e,q)$. The trivial transitions (q,e,q) may be inserted/deleted wherever q occurs in V (without changing the path).

PART I

Uniqueness and existence of a minimal saturated automaton Sat(R).

3. Definitions: homomorphisms, saturation.

Definition 3.1: Given 2 semiautomata $\mathcal{A}_i = (Q_i, \Sigma, M_i)$ $i = 1,2$. ϕ: $Q_1 \to Q_2$ is called a transition homomorphism from $\mathcal{A}_1$ to $\mathcal{A}_2$ iff

$(q,a,q') \in M_1 \Rightarrow (\phi(q), a, \phi(q')) \in M_2$ (or $(\phi(q),a,\phi(q'))=(q'',e,q'')$).

Such a ϕ will induce a mapping from the paths in $\mathcal{A}_1$ to the paths in $\mathcal{A}_2$, and we write $\phi(q^0,a^1,\ldots,q^i,\ldots,a^k,q^k) = (\phi(q^0),a^1,\ldots,\phi(q^i),\ldots,a^k,\phi(q^k))$.

Definition 3.2: Given $\mathcal{A}_i = (Q_i, \Sigma, M_i, S_i, F_i)$ $i=1,2$. ϕ: $Q_1 \to Q_2$ is an (automaton) homomorphism from $\mathcal{A}_1$ to $\mathcal{A}_2$ iff

a) ϕ is a transition homomorphism from (Q_1,Σ,M_1) to (Q_2,Σ,M_2)

b) $q \in S_1 \Rightarrow \phi(q) \in S_2$

c) $q \in F_1 \Rightarrow \phi(q) \in F_2$.

Such a ϕ will transform accepting paths for w in $\mathcal{A}_1$ to accepting paths for w in $\mathcal{A}_2$.

Definition 3.3: An automaton $\mathcal{A}' = (Q', \Sigma, M', S', F')$ is a subautomaton of $\mathcal{A} = (Q,\Sigma,M,S,F)$ iff $Q' \subseteq Q$, $M' \subseteq M$, $S' \subseteq S$, $F' \subseteq F$. We then write $\mathcal{A}' \subseteq \mathcal{A}$.

When ϕ is a homomorphism from $\mathcal{A}_1$ to $\mathcal{A}_2$, the image of $\mathcal{A}_1$ via ϕ is denoted $\phi(\mathcal{A}_1)$ and $\phi(\mathcal{A}_1) \subseteq \mathcal{A}_2$.

<u>Lemma 3.1</u>: $T(\mathcal{A}_1) \subseteq T(\phi(\mathcal{A}_1)) \subseteq T(\mathcal{A}_2)$ whenever ϕ is a homomorphism from $\mathcal{A}_1$ to $\mathcal{A}_2$.

<u>Remark</u>: McNaughton [7] defines homomorphism similar to our transition homomorphism, but there is one difference: He permits $(q,a,q') \in M_1$ to be transformed to $\phi(q) = \phi(q')$ even when $a \neq e$. Then $\phi(q^0,a^1,\ldots,a^k,q^k) = (\phi(q^0),b^1,\ldots,b^k,\phi(q^k))$ where

$$b_i = \begin{cases} a^i & \text{if } (\phi(q^{i-1}),\ a^i,\ \phi(q^i)) \in M_2 \\ e & \text{otherwise (then } \phi(q^{i-1}) = \phi(q^i)\ a^i \neq e) \end{cases}$$

In this case P and $\phi(P)$ will <u>not</u> span the same word.

But we regard the word spanned by a path as an important property of the path, so we want homomorphisms to preserve words and to make lemma 3.1. true.

<u>Definition 3.4</u>. An <u>isomorphism</u> between $\mathcal{A}_1$ and $\mathcal{A}_2$ is a homomorphism which also satisfies:

- ϕ is a bijection between Q_1 and Q_2
- ϕ induces a bijection between M_1 and M_2.

<u>Definition 3.5</u>. An automaton $\mathcal{A}$ is <u>saturated</u> (with respect to R) iff

1) $\mathcal{A}$ accepts R;
2) For all automata $\mathcal{A}'$ accepting (a subset of) R, there is a homomorphism ϕ from $\mathcal{A}'$ to $\mathcal{A}$.

$\mathcal{A} = (Q, \Sigma, M, S_0, F_0)$ is said to be minimal saturated (relative to R) if $\mathcal{A}$ is saturated and minimal in the class, i.e:

For all $\mathcal{A}''$ satisfying 1) and 2)

we have $\# Q \leqslant \# Q''$

and $\# M \leqslant \# M''$

Lemma 3.2. If $\mathcal{A}_1$ is saturated, $T(\mathcal{A}_2) = R$ and ϕ is a homomorphism from $\mathcal{A}_1$ to $\mathcal{A}_2$ then $\phi(\mathcal{A}_1)$ is saturated, and so is $\mathcal{A}_2$.

Proof: Immediate.

Proposition 3.3. (Uniqueness) Let $\mathcal{A}$ and $\mathcal{A}'$ be minimal saturated automata relative to R. Then there is an isomorphism between $\mathcal{A}$ and $\mathcal{A}'$.

Proof. Write $\mathcal{A} = (Q, \Sigma, M, S, F)$, $\mathcal{A}' = (Q', \Sigma, M', S', F')$. Since both $\mathcal{A}$ and $\mathcal{A}'$ are minimal $\# Q = \# Q'$ and $\# M = \# M'$. Since $\mathcal{A}'$ is saturated and $T(\mathcal{A}) = R$, there exist a $g: \mathcal{A} \to \mathcal{A}'$. By lemma 3.2. $g(\mathcal{A})$ is also saturated, so g must be onto Q', that is g is a bijection between Q and Q'. g will also give a bijection between M and M'.

This unique saturated automaton will be denoted Sat(R).

4. Maximal pairs. The construction of Sat(R)

Before we give the formal definition of Sat(R), we will give an example which shows that saturated automata (though not minimal) have been considered before. From this example it turns out that we only have to delete some of the states in order to obtain Sat(R).

Ex.4.1 (From Cohen and Brzozowski [2])

Given $\mathrm{Det}^-(R) = (\hat{P}, \Sigma, \delta_D, p_e, F_D)$

Define the subsetautomaton of order k

$$\mathcal{A}_k(R) = (P^k, \Sigma, M_k, P_0^k, F^k)$$

where $P^k = \{P'_{(i)} \mid \emptyset \neq P' \subseteq \hat{P} \qquad 1 \leq i \leq k\}$

$P_0^k = \{P'_{(i)} \mid p_e \in P' \qquad 1 \leq i \leq k\}$

$F_1^k = \{P'_{(i)} \mid P' \subseteq F_D \qquad 1 \leq i \leq k\}$

$(P'_{(i)}, a, P''_{(j)}) \in M_k \iff \delta_D(P', a) \subseteq P'', \; a \in \Sigma.$

Define the R-projection function $f_R^{\mathcal{A}'} : Q' \to 2^{\hat{P}}$ by $f_R^{\mathcal{A}'}(q') = \delta_D(p_e, Pr^{\mathcal{A}'}(q'))$.

$f_R^{\mathcal{A}'}$ turns out to be a homomorphism from $\mathcal{A}'$ to $\mathcal{A}_1(R)$ (or $\mathcal{A}_k(R)$) whenever $T(\mathcal{A}') = R$ (Lemma 6.2, 6.3 in [2]) (in fact $T(\mathcal{A}') \subseteq R$ suffices). This shows that $\mathcal{A}_1(R)$ (and $\mathcal{A}_k(R)$) are saturated automata.

<u>Remark</u>: Strictly speaking $f_R^{\mathcal{A}'}$ is a homomorphism only when $\mathcal{A}'$ is without e-transitions and without dead and inaccessible states. However $\mathcal{A}_k(R)$ can easily be modified by starting with Det(R) (possibly with a dead state) and define:

$$P^k = \{P'_{(i)} \mid \emptyset \subseteq P' \subseteq \hat{P} \;,\; 1 \leq i \leq k\}$$

$$(P'_{(i)}, a, P''_{(j)}) \in M_k \;\text{ iff }\; \delta_D(P', a) \subset P'', \; a \in \Sigma \cup \{e\}$$

This modified $\mathcal{A}_k(R)$ will be saturated in our sense.
When we regard $\hat{P}$ as $\{[u]_R \mid u \in \Sigma^*\}$ the states in $\mathcal{A}_k(R)$ corresponds to different unions of such equivalence classes.

In order to obtain Sat(R) it is necessary to delete some states in $\mathcal{A}_1(R)$.

The following construction of Sat(R) is due to Stål Aanderaa:

<u>Definition 4.1</u>: Given $P, Q \subseteq \Sigma^*$, and R a language over Σ^*.

Let $R::P = \{v \in \Sigma^* \mid P\{v\} \subseteq R\}$

$R:Q = \{v \in \Sigma^* \mid \{v\}Q \subseteq R\}$

We say that (P,Q) is a <u>pair</u> relative to R iff $PQ \subseteq R$. We say that (P,Q) is a <u>maximal pair</u> relative to R iff

1) $PQ \subseteq R$
2) $\forall v \in \Sigma^* (\{v\}Q \subseteq R \Rightarrow v \in P)$ i.e. $P \supseteq R:Q$
3) $\forall v \in \Sigma^* (P\{v\} \subseteq R \Rightarrow v \in Q)$ i.e. $Q \supseteq R::P$.

This means that the pair (P,Q) is maximal iff neither the first nor second component of (P,Q) can be further extended preserving the property of being a pair. Observe the following equalities:

$R::P = \bigcap_{w \in P} w \backslash R \quad R:Q = \bigcap_{v \in Q} R/v.$

We have the following equivalent characterization of (P,Q) beeing a maximal pair:

<u>Definition 4.2</u>: Let $\bar{P} = R:(R::P)$ and $\tilde{Q} = R::(R:Q)$

<u>Proposition 4.1</u>: The following are equivalent:

1) (P,Q) is a maximal pair relative to R
2) (P,Q) is a pair, $P = R:Q$ and $Q = R::P$
3) $P = \bar{P}$ and $Q = R::P$
4) $Q = \tilde{Q}$ and $P = R:Q$.

<u>Example 4.2</u>: Given $\mathcal{A}$ such that $T(\mathcal{A}) \subseteq R$. For all q in $\mathcal{A}$, $Pr^{\mathcal{A}}(q)Sc^{\mathcal{A}}(q) \subseteq T(\mathcal{A}) \subseteq R$. So $(Pr^{\mathcal{A}}(q), Sc^{\mathcal{A}}(q))$ is a pair with respect to R, and every pair (P,Q) with respect to R can be extended to a maximal pair; two possibilities are $(\bar{P}, R::P)$ or $(R:Q, \tilde{Q})$.

<u>Definition 4.3</u>: Given a maximal pair $r = (P',Q')$, we write P (Q)

for the projection maps, that is

$$P(r) = P' \quad \text{and} \quad Q(r) = Q'$$

Proposition 4.2: For all $P,Q \subseteq \Sigma^*$ and all $R \subseteq \Sigma^*$

1) $R: Q$ consists of a union of $\overset{D}{\sim}$ equivalence classes.

2) $R:: P$ consists of a union of $\overset{B}{\sim}$ equivalence classes.

Proof:

1) Remember $\overset{D}{\sim}$ is defined by: $u \overset{D}{\sim} v$ iff $\forall w \in \Sigma^*(uw \in R \Leftrightarrow vw \in R)$. We will show $u \in R: Q \Leftrightarrow [u] \subseteq R: Q$. For abritrary $v \in [u]$ we have:

$$\forall w \in \Sigma^*(uw \in R \Leftrightarrow vw \in R)$$
$$\Rightarrow \quad \forall w \in Q(uw \in R \Leftrightarrow vw \in R)$$
$$\Rightarrow \quad (\forall w \in Q \; uw \in R) \Leftrightarrow (\forall w \in Q \; vw \in R)$$
$$\Leftrightarrow \quad (u \in R: Q \Leftrightarrow v \in R:Q)$$

This shows $u \in R: Q \Leftrightarrow [u] \subseteq R: Q$.

2) follows by duality.

Corollary 4.3: If R is regular,

$$R: Q = \bigcup_{p' \in P'} Pr^{Det(R)}(p') \quad \text{and} \quad R: P = \bigcup_{q' \in Q'} Sc^{BDet(R)}(q')$$

where P' and Q' are suitable subsets of $\hat{P}$ and $\hat{Q}$.

Corollary 4.4: If R is regular, there is only a finite number of maximal pairs.

In fact we also have the converse of 4.4: Whenever we have a finite set of the maximal pairs for a given language R, we can construct an automaton $\mathcal{A}_R$ accepting R, showing that R is regular.

Definition 4.3: $\mathcal{A}_R = (K_R, \Sigma, M_R, S_R, F_R)$ where

$K_R = \{r_i = (P_i, Q_i) \quad i=1,\ldots,N\}$ = the maximal pairs.

$S_R=\{r_i | e \in P_i\}$ $F_R=\{r_j | P_j \subseteq R\}$

$(r_i, a, r_j) \in M_k$ iff $P_i\{a\} \subseteq P_j$, $a \in \Sigma \cup \{e\}$

(This corresponds to the definition of $\mathcal{A}_1(R)$ in example 4.1, except that we do not consider all $P' \subseteq \hat{P}$, only those where $P'=\bar{P}'$.)

Note: We have always the following maximal pairs:

$\underline{\text{top}} = (R::\Sigma^*, \Sigma^*)$, $\underline{\text{bottom}} = (\Sigma^*, R:\Sigma^*)$.

And we have:

top $\in F_R$ and (top, a, r) $\in M_R$, $\forall r \in K_R$, $\forall a \in \Sigma \cup \{e\}$.

bottom $\in S_R$ and (r, a, bottom) $\in M_R$, $\forall r \in K_R$, $\forall a \in \Sigma \cup \{e\}$.

This shows that the transitions out of top and into bottom are (for most purposes) useless.

Often bottom is equal to $(\Sigma^*, \emptyset)$, and then bottom is the dead state; and when top is equal to $(\emptyset, \Sigma^*)$, top is the inaccessible state (See prop.4.10).

Before we are able to show that $T(\mathcal{A}_R) = R$ we need some properties of : and :: division and - and ~ closure.

Lemma 4.5: 1) $P_1 \supset P_2 \Rightarrow R::P_1 \subseteq R::P_2$

$Q_1 \supset Q_2 \Rightarrow R:Q_1 \subseteq R:Q_2$

2) $P_1 \subset P_2 \Rightarrow \bar{P}_1 \subseteq \bar{P}_2$

$Q_1 \subset Q_2 \Rightarrow \tilde{Q}_1 \subseteq \tilde{Q}_2$

Lemma 4.6: 1) $P \subseteq \bar{P}$ $\quad Q \subseteq \tilde{Q}$

2) $R::P = R::\bar{P}$ $\quad R:Q = R:\tilde{Q}$

3) $R:Q = \overline{R:Q}$ $\quad R::P = R::P$

4) $\bar{\bar{P}} = \bar{P}$ $\quad \tilde{\tilde{Q}}=\tilde{Q}$

5) $P_1 \subseteq \bar{P}_2 \Rightarrow \bar{P}_1 \subseteq \bar{P}_2$

$Q_1 \subseteq \tilde{Q}_2 \Rightarrow \tilde{Q}_1 \subseteq \tilde{Q}_2$

6) $\bar{P} = \bigcap_{\bar{P}_1 \supseteq P} \bar{P}_1 \qquad \tilde{Q} = \bigcap_{\tilde{Q}_1 \supseteq Q} \tilde{Q}_1$

7) $PQ \subseteq R \Leftrightarrow \bar{P}Q \subseteq R \Leftrightarrow P\tilde{Q} \subseteq R \Leftrightarrow \bar{P}\tilde{Q} \subseteq R$

8) $\overline{\{w\}} = \overline{[w]} \qquad \widetilde{\{w\}} = \widetilde{\langle w \rangle}$

<u>Proof:</u> 1) Immidiate since $P(R::P) \subseteq R$

2) From 4.5.1) with $\bar{P} \supset P$ we get $R::\bar{P} \subseteq R::P$
For the opposite: If $v \notin R::\bar{P}$ then $\bar{P}\{v\} \subseteq R$. But since $\bar{P} = R:(R::P)$, $\bar{P}(R::P) \subseteq R$, this shows that $v \notin R::\bar{P} \Rightarrow v \notin (R::P)$.

3) $\overline{R:Q} = R:(R::(R:Q)) = R:\tilde{Q} = R:Q$ by 2)

4) $\bar{\bar{P}} = R:(R:\bar{P}) = R:(R:P) = \bar{P}$ by 2)

5) from 4.5.2) and 4)

6) from 5)

7) By 2) if $PQ \subseteq R$ then $\bar{P}Q \subseteq R$ and $P\tilde{Q} \subseteq R$ a second application gives $\bar{P}\tilde{Q} \subseteq R$. The implications to the left are immediate from 1)

8) From the proof of prop. 4.2.

<u>Lemma 4.7.</u> Given (P_1, Q_1) and (P_2, Q_2) maximal pairs with respect to R and $u \in \Sigma^*$.

1) The following are equivalent:

i) $P_1\{u\} Q_2 \subseteq R$

ii) $P_1\{u\} \subseteq P_2$

iii) $\{u\}Q_2 \subseteq P_1$

2) $P_1 \subsetneqq P_2 \Leftrightarrow Q_1 \supsetneqq Q_2$

3) $P_1 \subseteq R \Leftrightarrow e \in Q_1$, $Q_1 \subseteq R \Leftrightarrow e \in P_1$.

Proof: Immediate.

Lemma 4.8. For all $P_1, Q \subseteq \Sigma^*$ $u \in \Sigma^*$ we have the following:

$$\bar{P}\{u\} \subseteq (\overline{P\{u\}})$$
$$\{u\}\tilde{Q} \subseteq (\widetilde{\{u\}Q})$$

Proof: Let $(P_1, Q_1) = (\bar{P}, R::P)$ and $(P^u, Q^u) = (\overline{P\{u\}}, R:(P\{u\}))$

These are maximal pairs and

$\{u\}Q^u = \{u\}(R:P\{u\}) = \{u\}\{w\in\Sigma^* \mid P\{u\}\{w\}\subseteq R\} \subseteq \{v\in\Sigma^* \mid P\{v\}\subseteq R\} = R::P = Q_1.$

By 4.7.1) $\{u\}Q^u \subseteq Q_1$ is equivalent to $P_1\{u\}\subseteq P^u$, that is $\bar{P}\{u\}\subseteq\overline{P\{u\}}$.

We are now ready to show that $T(\mathcal{A}_R) = R$:

Proposition 4.9: $T(\mathcal{A}_R, r_i, r_j) = \{u \mid P_i\{u\}Q_j \subseteq R\}$ where $r_i = (P_i, Q_i)$, $r_j = (P_j, Q_j)$.

Proof of $\subseteq$: By an easy induction.

Proof of $\supseteq$: Suppose $P_i\{u\}Q_j \subseteq R$. We will show $u \in T(\quad_R, r_i, r_j)$ by induction on the length of u.

$u \in \Sigma\cup\{e\}$: By definition $(r_i, u, r_j) \in M_R$.

$u = u'a$ $a\in\Sigma$: $P_1\{u\}Q_j \subseteq R$ means $P_i\{u'\}\{a\}Q_j \subseteq R$

Extend the pair $(P_i\{u'\}, \{a\}Q_j)$ to a maximal pair by $r' = (\overline{P_i\{u'\}}, R::(P_i\{u'\}))$.

This gives: 1) $P_i\{u\} \subseteq \overline{P_i\{u'\}} = P(r') = R: Q(r')$

and 2) $\{a\}Q_j \subseteq R::(P_i\{u'\}) = Q(r') = R::P(r')$.

1) is equivalent to $P_i\{u'\}Q(r') \subseteq R$ which by induction gives $u' \in T(\mathcal{A}_R, r_i, r')$

2) is equivalent to $P(r')\{a\}Q_j \subseteq R$ that is $(r', a, r_j) \in M_R$.

This shows that $u=u'a$ is spanned via a path $(r_i,\ldots u'\ldots,r',a,r_j)$.

This proof is a typical proof by induction on the length of a word (or the length of a path). In the rest of this paper such proofs will often be omitted.

<u>Proposition 4.10</u> $T(\mathcal{A}_R, S_R, r_j) = P_j$ and $T(\mathcal{A}_R, r_i, R_R) = Q_i$

<u>Proof</u> of $\subseteq$: $T(\ _R, S_R, r_j) = \bigcup_{e \in P_i} T(\ _R, r_i, r_j)$

$$= \bigcup_{e \in P_i} \{u | P_i\{u\}Q_j \subseteq R\} \subseteq \{u | \{e\}\{u\}Q_j \subseteq R\} = R: Q_j = P_j.$$

<u>Proof</u> of $\supseteq$: By induction on the length of u.

<u>Corollary 4.11</u> $T(\mathcal{A}_R) \subseteq R$.

<u>Proof</u>: $T(\mathcal{A}_R) = \bigcup_{r_i \in K_R} T(\mathcal{A}_R, S_R, r_i) T(\mathcal{A}_R, r_i, F_R) = \bigcup_{r_i \in K_R} P_i Q_i \subseteq R.$

In fact, $T(\mathcal{A}_R) = R$. This can be proved using the method of prop. 4.9 and 4.10, but we will instead show that $\mathcal{A}_R$ satisfies the homomorphism requirement for a saturated automaton, and from that fact deduce that $R \subseteq T(\mathcal{A}_R)$.

<u>Definition 4.4</u>: Given an automaton $\mathcal{A} = (Q, \Sigma, M, S_0, F)$ define

$f_i: Q \to K_R \quad i = 1,2$ by

$f_1(q) = (\overline{Pr^{\mathcal{A}}(q)}, R::Pr^{\mathcal{A}}(q))$

$f_2(q) = (R:Sc^{\mathcal{A}}(q), \widetilde{Sc^{\mathcal{A}}(q)})$

<u>Proposition 4.12</u>: If $T(\mathcal{A}) \subseteq R$ then $f_1^{\mathcal{A}}$ and $f_2^{\mathcal{A}}$ are homomorphisms from $\mathcal{A}$ into $\mathcal{A}_R$.

<u>Proof</u> (for f_1):

<u>When $q \in S$</u>: Then $e \in Pr^{\mathcal{A}}(q) \subseteq \overline{Pr\ (q)} = P(\ f_1(p))$, which shows $f_1(p) \in S_R$.

<u>When $q \in F$</u>: Then $Pr^{\mathcal{A}}(q) \subseteq T(\mathcal{A}) \subseteq R$, and by 4.6.7 with $Q = \{e\}$ this implies $\overline{Pr(q)} \subseteq R$. Which shows $P(f_1(q)) \subseteq R$ i.e. $f_1(q) \in F_R$.

<u>When $(q, a, q') \in M$</u> : Then $T(\mathcal{A}, S, q)\{a\} \subseteq T(\mathcal{A}, S, q')$. This implies (by lemma 4.8)

$$\overline{T(\mathcal{A}, S, q)}\{a\} \subseteq \overline{T(\mathcal{A}, S, q)\{a\}} \subseteq \overline{T(\mathcal{A}, S, q')}$$

i.e. $P(f_1(q))\{a\} \subseteq P(f_1(q')$. This shows $(f_1(q), a, f_1(q')) \in M_R$.

<u>Convention:</u> We will often write f_1 and $Pr(q)$ instead of f_1 $Pr\ (q)$ etc. when the reference to $\mathcal{A}$ is understood. f_1 and $Pr(p)$ often refers to $Det(R)$ and f_2 and $Sc(q)$ often refers to $BDet(R)$.

<u>Corollary 4.13</u>: $T(\mathcal{A}_R) = R$ and $\mathcal{A}_R$ is saturated.

<u>Proof</u>: f_1: $Det(R) \to \mathcal{A}_R$ shows

$$R = T(Det(R)) \subseteq T(f_1(\mathcal{A}_R)) \subseteq R$$

The rest is by 4.11 and 4.12.

<u>Lemma 4.14</u>: If $g: \mathcal{A}_R \to \mathcal{A}_R$ is a homomorphism then g is the identity.

<u>Proof</u>:

$P(r) = T(\mathcal{A}_R, S_R, r) \subseteq T(g(\mathcal{A}_R), g(S_R), g(r)) \subseteq T(\mathcal{A}_R, S_R, g(r)) = P(g(r))$.

Likewise $Q(r) \subseteq Q(g(r))$, which is equivalent to $P(r) \supseteq P(g(r))$. This gives $P(r) = P(g(r))$, i.e. $r = g(r)$.

<u>Theorem 4.15</u>: $\mathcal{A}_R = Sat(R)$.

<u>Proof</u>: Minimality follows from 4.14 and lemma 3.2.

5 Reduced automaton matrix. How to compute Sat(R)

We have seen that for all maximal pairs $r = (P,Q)$ P and Q can be written as

$$P = [u_{i_1}] \cup \ldots \cup [u_{i_n}]$$

$$Q = \langle v_{j_1} \rangle \cup \ldots \cup \langle v_{j_m} \rangle$$

Since $\overset{D}{\sim}$ ($\overset{B}{\sim}$) equivalence classes correspond to states $p \in \hat{P}$ ($q \in \hat{Q}$) in Det(R) (BDet(R)) such that

$$[u] = Pr(p_u) \quad \text{where} \quad p_u = \delta_D(p_e, u)$$

$$\langle v \rangle = Sc(q_v) \quad \text{where} \quad q_v = \overleftarrow{\delta}_B(q_e, \overleftarrow{v})$$

we can make the following definition in order to simplify the tests whether $P = R:Q$ $P=\overline{P}$ etc.

<u>Definition 5.1</u>. The reduced automaton matrix (RAM) (relative to R) is defined as a $\#\hat{P} \times \#\hat{Q}$ matrix

$$\text{where} \quad RAM(p,q) = \begin{cases} + \text{ if } & Pr(p)Sc(q) \subseteq R \\ - \text{ otherwise} \end{cases}$$

If Det(R) and BDet(R) are computed, choose one $w_p \in Pr(p)$ and one $v_q \in Sc(q)$; then:

$$Pr(p)Sc(q) \subseteq R \iff [w_p]\langle v_q \rangle \subseteq R \iff w_p v_q \in R.$$

This is easily tested. If we just are given an automaton $\mathcal{A}$ accepting R, Det(R) and $\overleftarrow{\text{BDet}}$(R) can be constructed as $\mathcal{D}(\mathcal{A})^\wedge$ and $(\mathcal{D}(\overleftarrow{\mathcal{A}}))^\wedge$. The reductions (given by the $^\wedge$-operators in definition 2.4) can be preformed in the following way: (See [5] where RAM and EAM are defined.)

<u>Definition 5.2</u>: Given $\mathcal{A} = (S, \Sigma, M, S_0, F)$. Construct $\mathcal{D}(\mathcal{A}) = (P, \Sigma, M', S_0', F')$ where $P \subseteq 2^S$, and $\mathcal{D}(\overleftarrow{\mathcal{A}}) = (Q, \Sigma, M'', S'', F'')$

where $Q \subseteq 2^S$. Define the elementary automaton matrix (EAM) (relative to $\mathcal{A}$) as a $\#P \times \#Q$ matrix

where $EAM(p,q) = \begin{cases} 1 & \text{if } p \cap q \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$

The reduction from $\mathcal{A}$ to $\mathcal{A}^{\wedge}$ and from $\mathcal{A}^{\leftarrow}$ to $\mathcal{A}^{\leftarrow\wedge}$ can be done by "merging" rows and columns with identical 0/1 patterns.

Each $[p] \in \hat{P}$ may be regarded as $\bigcup_{p' \sim p} p' \subseteq 2^S$, and similar with $[q] \in \hat{Q}$. With these notations RAM is defined in [5] as:

$$RAM([p],\ [q]) = \begin{cases} 1 & \text{if } [p] \cap [q] \neq \emptyset \\ 0 & \text{otherwise} \end{cases}$$

<u>Proposition 5.1</u>: This definition of RAM is equivalent to definition 5.1.

<u>Proof</u> (sketch): Since $Det(R)$ defined by means of Myhill-Nerodes $\overset{D}{\sim}$-equivalence and $\mathfrak{D}(\mathcal{A})^{\wedge}$ are isomorphic.

In [5] also grids and prime grids are defined:

<u>Definition 5.3</u>: $g = (P_I;\ Q_J)$ where $P_I \subseteq \hat{P}$ $Q_J \subseteq \hat{Q}$ is said to be a <u>grid</u> if

$$RAM(p_i, q_j) = 1 \quad \forall p_i \in P_I \quad \forall q_j \in Q_J$$

g is a <u>prime grid</u> if neither component can be further extended preserving the property of being a grid.

Maximal pairs and prime grids are corresponding notions, and all maximal pairs can be found by means of RAM.

If the maximal pair $r = (P,Q)$ corresponds to the prime grid $(P_I;Q_J)$ and $r' = (P',Q')$ corresponds to $(P_{I'};\ Q_{J'})$, the transitions in $Sat(R)$ can be computed as

$$M_R(r,a) = \{r' \mid P(r)\{a\} \subseteq P(r')\}$$
$$= \bigcap_{p_i \in P_I} \{r' \mid Pr(p_i)\{a\} \subseteq \bigcup_{p_i' \in P_{I'}} Pr(p_i')\}$$
$$= \bigcap_{p_i \in P_I} \{r' \mid \delta_D(p_i,a) \in P_{I'}\} \qquad a \in \Sigma \cup \{e\}$$

This shows that M_R can be computed when we know RAM and δ_D by using the above intersection rule.

Remark: This intersection rule shows the strong connection between Sat(R) and the automaton $\mathcal{J}$ = I(Z, f, Det(R)) defined by Kameda and Weiner in [5]:

Given some prime grids Z (the states of $\mathcal{J}$) define $f: P \to 2^Z$ by $f(p) = \{(P_I; Q_J) \in Z \mid p_i \in P_I\}$.

The transitions, denoted N in $\mathcal{J}$ are defined by

$$N(z,a) = \bigcap_{p \mid z \in f(p)} f(\delta_D(p,a)).$$

If $z = (P_I; Q_J)$ this gives $N((P_I; Q_J), a) = \bigcap_{p_i \in P_I} f(\delta_D(p_i, a)) =$

$$= \bigcap_{p_i \in P_I} \{z' = \{P_{I'}; Q_{J'}) \mid \delta_D(p_i,a) \in P_{I'}\}, \quad a \in \Sigma.$$

This corresponds exactly to the intersection rule in Sat(R), and by the correspondence between prime grids and maximal pairs we have:

$$I(Z,A, Det(R)) \approx \mathcal{A}_Z \subseteq Sat(R)$$

where $\mathcal{A}_Z = (K_R \cap K_Z, \Sigma, M_R \cap (K_Z \times \Sigma \times K_Z), S_R \cap K_Z, F_R \cap K_Z)$ and K_Z is the set of maximal pairs corresponding to the set of prime grids Z.

Kameda and Weiner was interested in minimal, nondeterministic automata with respect to R, and from the homomorphism property of

Sat(R), it is immediate that such an automaton can be found by searching for subautomta of Sat(R). This is in essence their algorithm (although they never constructed all of Sat(R)).

Ex.5.1. Let R=T($\mathcal{A}$) where $\mathcal{A}$ is given in fig.5.1.1).

The transition tables for $\mathcal{A}$ and $\mathcal{A}^+$ are shown in fig. 5.1.2). From these the transition tables for $\mathcal{D}(\mathcal{A})$ and $\mathcal{D}(\mathcal{A}^+)$ are computed (fig.5.1.3).

Fig 5.1.1)

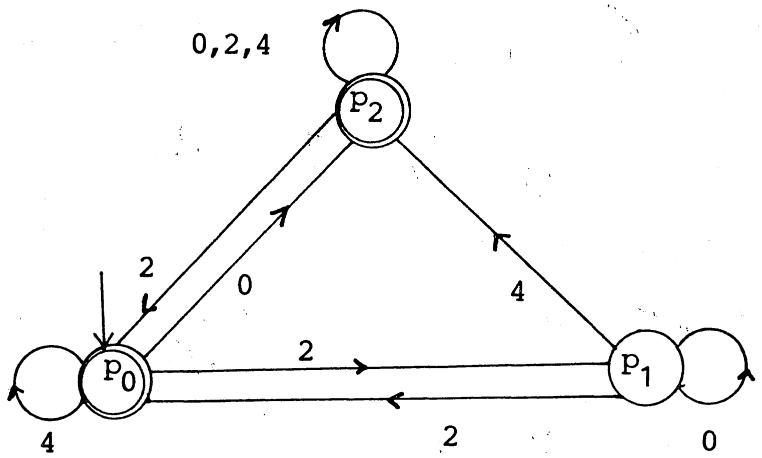


Fig 5.1.2)

$\mathcal{A}$	0	2	4
p_0	p_2	p_1	p_1
p_1	p_1	p_0	p_2
p_2	p_2	p_{02}	p_2

0	2	4	$\mathcal{A}^+$
-	p_{12}	p_0	p_0'
p_1	p_0	-	p_1
p_{02}	p_2	p_{12}	p_2

Fig 5.1.3)

$\mathcal{D}(\mathcal{A})$	0	2	4
p_0	p_2	p_1	p_0
p_1	p_1	p_0	p_2
p_2	p_2	p_{02}	p_2
p_{02}	p_2	p_{012}	p_{02}
p_{012}	p_{12}	p_{012}	p_{02}
p_{012}	p_{12}	p_{02}	p_2

0	2	4	$\mathcal{D}(\mathcal{A}^+)$
p_{02}	p_{12}	p_{012}	p_{02}
p_{012}	p_{02}	p_{12}	p_{12}
p_{12}	p_{012}	p_{012}	p_{012}

EAM($\mathcal{A}$) is shown in fig.5.1.4), and we see that $\{p_0\} \sim \{p_0, p_2\} \sim \{p_0, p_1, p_2\} \sim \{p_1, p_2\}$ in $\mathfrak{D}(\mathcal{A})$. We also see that $\mathfrak{D}(\mathcal{A})$ is reduced$(=\overleftarrow{\mathrm{BDet}(R)})$. By merging the rows in EAM, we get RAM, shown in fig. 5.1.5).

The transition tables for Det(R) and BDet(R) are shown in fig. 5.1.6).

We compute f_1: Det(R) $\rightarrow$ Sat(R)

Note: By the isomorphism between maximal pairs and prime grids we will write $R::p_i = \{q^1,\ldots,q^k\}$ instead of $R::[w_i] = \langle v^1\rangle \cup \cdots \cup \langle v^k\rangle$, etc.

This gives

$R::p_0 = \{q_a, q_c\}$, $R:\{q_a, q_c\} = \{p_0,p_2\}$,

$R::p_1 = \{q_b, q_c\}$, $R:\{q_b, q_c\} = \{p_1,p_3\}$,

$R::p_3 = \{q_a,q_b,q_c\}$, $R:\{q_a,q_b,q_c\} = \{p_3\}$,

so $f_1(p_0) = (\{p_0,p_3\}, \{q_a,q_c\}) = r_0$
$f_1(p_1) = (\{p_1,p_3\}, \{q_b,q_c\}) = r_1$
$f_1(p_3) = (\{p_3\}, \{q_a,q_b,q_c\}) = r_3$

Similarly f_2: BDet(R) $\rightarrow$ Sat(R) can be computed, and we get a new maximal pair $r_4 = (\{p_0, p_1, p_3\}, \{q_c\})$.

It can be verified r_1, r_2, r_3, r_4 are the only maximal pairs. (See also the algorithm on p.36 of section 8.)

Fig.5.1.4)

EAM	p_{02}	p_{12}	p_{012}
p_0	+	−	+
p_1	−	+	+
p_2	+	+	+
p_{02}	+	+	+
p_{012}	+	+	+
p_{12}	+	+	+

Fig.5.1.5)

RAM	q_a p_{01}	q_b p_{12}	q_c p_{012}
p_0	+	−	+
p_1	−	+	+
$p_3 = p_{012}$	+	+	+

Fig.5.1.6)

Det(R)	0	2	4
p_0	p_3	p_1	p_0
p_1	p_1	p_0	p_3
p_3	p_3	p_3	p_3

0	2	4	BDet(R)
q_a	q_b	q_c	q_a
q_e	q_a	q_b	q_b
q_c	q_c	q_e	q_c

The transiton in table for Sat(R) is computed from RAM and δ_D in the following way: First make a small table indicating if "$\{p_i\}\{a\}\{q_j\}$" $\subseteq R$ (really if $Pr^{Det(R)}(p_i)\{a\}\ Sc^{BDet(r)}(q_j) \subseteq R$ i.e. $RAM(\delta_D(p_i,a),\ q_j) = +)$.

Then use the intersection rule to extend this table to "$P\{a\}Q$" $\subseteq R$ for all $P \subseteq \hat{P}$ $Q \subseteq \hat{Q}$ which represents maximal pairs. This is shown in fig. 5.1.7). The lower right corner in 5.1.7) shows the transitons in Sat(R).

$$S_R = \{r_i | e \in P(r_i)\}$$

$$= \{r_i | p_0 \in \text{ the representation of } P(r_i)\} = \{r_0, r_4\}$$

$$F_R = \{r_i | P(r_i) \subseteq R\} = \{r_i | e \in Q(r_i)\}$$

$$= \{r_i | q_a \in \text{ the representation of } Q(r_i)\} = \{r_0, r_3\}$$

$$r_3 = (R\colon \Sigma^*,\ \Sigma^*) = (\{p_3\},\ \{q_a,\ q_b,\ q_c\}) = (\{p_3\},\ \hat{Q})$$

The modified Sat(R) without "useless" transitions are shown in fig. 5.1.9). The "basic" part of Sat(R) (see def. 6.3) are shown in fig 5.1.10).

Fig.5.1.7)

	a	$\delta_D(p_i,a)$	q_a	q_b	q_c	r_0 $\{q_a,q_c\}$	r_1 $\{q_b,q_c\}$	r_3 $\{q_a,q_b,q_c\}$	r_4 $\{q_c\}$
p_0	e	p_0	+	–	+				
	0	p_3	+	+	+				
	2	p_1	–	+	+				
	4	p_1	+	–	+				
p_1	e	p_1	–	+	+				
	0	p_1	–	+	+				
	2	p_0	+	–	+				
	4	p_3	+	+	+				
p_3	e	p_3	+	+	+				
	0	p_3	+	+	+				
	2	p_3	+	+	+				
	4	p_3	+	+	+				
r_0 $\{p_0,p_3\}$	e		+	–	+	+	–	–	+
	0		+	–	+	+	–	–	+
	2		–	+	+	–	+	–	+
	4		+	–	+	+	–	–	+
r_1 $\{p_1,p_3\}$	e		–	+	+	–	+	–	+
	0		–	+	+	–	+	–	+
	2		+	–	+	+	–	–	+
	4		+	+	+	+	+	+	+
r_3 $\{p_3\}$	e		+	+	+	+	+	+	+
	0		+	+	+	+	+	+	+
	2		+	+	+	+	+	+	+
	4		+	+	+	+	+	+	+
r_4 $\{p_0,p_1,p_3\}$	e		–	–	+	–	–	–	+
	0		–	+	+	–	+	–	+
	2		–	–	+	–	–	–	+
	4		+	–	+	+	–	–	+

Fig. 5.1.8)

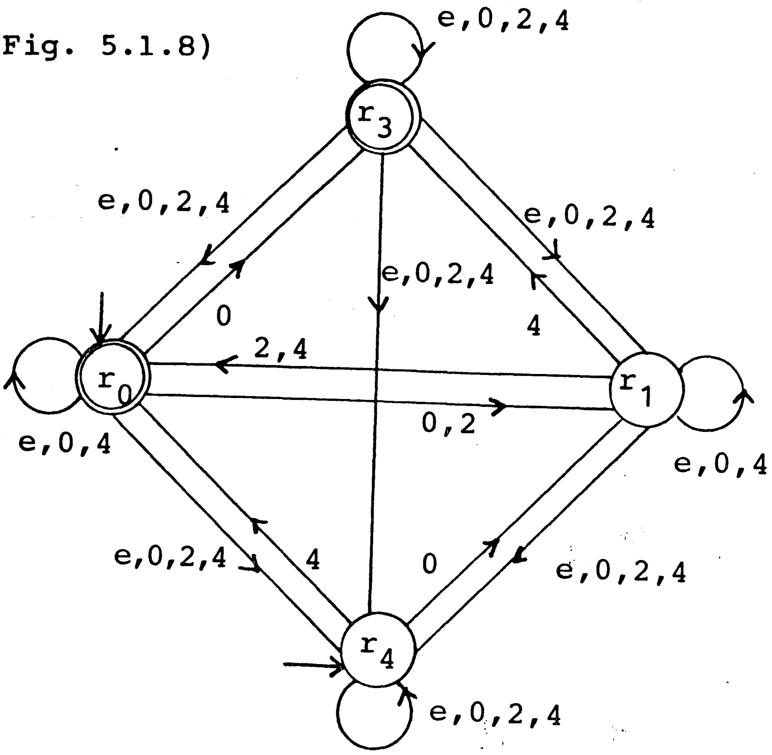


Fig. 5.1.9)

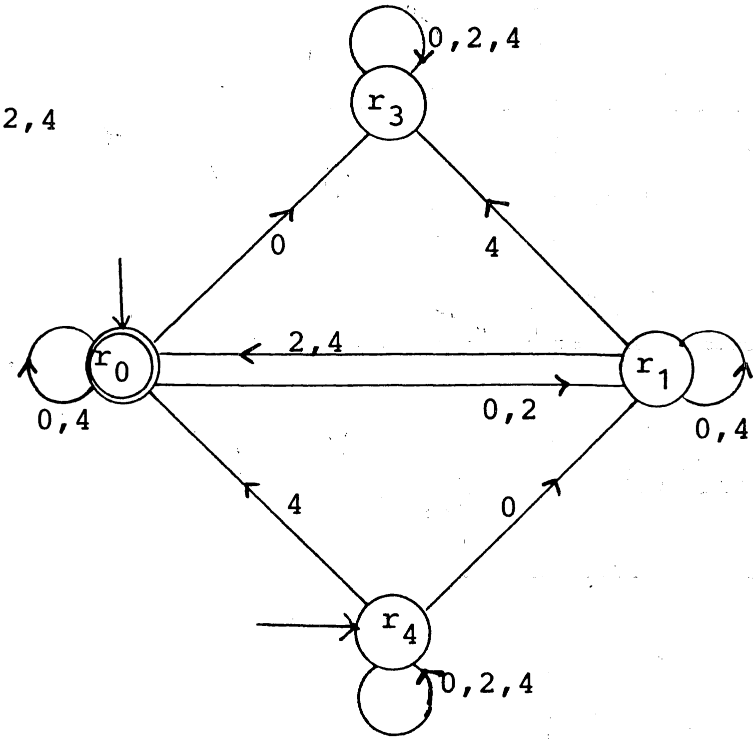
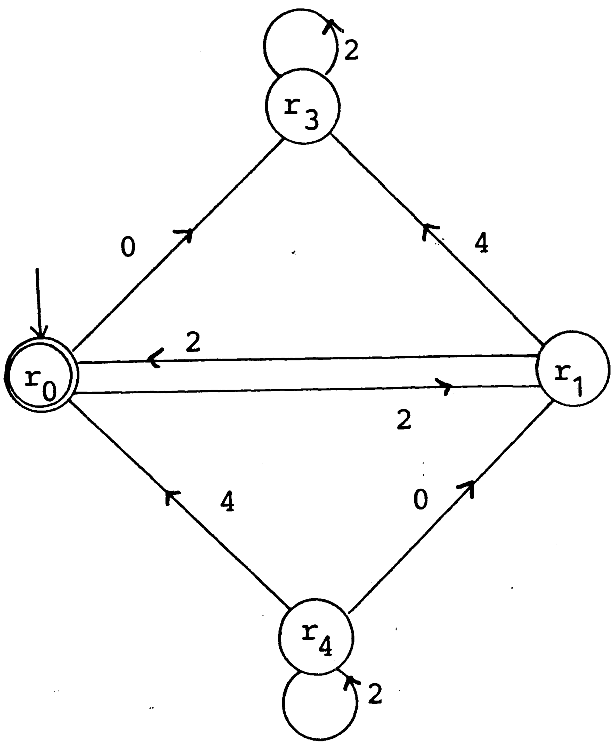


Fig. 5.1.10)



Ex. 5.2. Let $\mathcal{A} = \mathcal{A}_3 = \{q_1, q_2, q_3\}, \{0,1\}, M_3, q_1, q_3)$ where $(q_i, k, q_j) \in M_3 \Leftrightarrow i + k \equiv j \mod 3 (k=0,1,2)$. Let $R_3 = R = T(\mathcal{A})$. We see that $\mathcal{A}$ is forward and backward deterministic so $\mathcal{D}(\mathcal{A}) = \mathcal{A}$ and $\mathcal{D}(\overleftarrow{\mathcal{A}}) = \overleftarrow{\mathcal{A}}$. EAM($\mathcal{A}$) is shown in fig. 5.2.1), and we see that EAM($\mathcal{A}$) is reduced (i.e. EAM=RAM), so $\mathcal{A}$ = Det(R) = BDet(R).

We have the following maximal pairs: bottom = $(\Sigma^*, \emptyset)$, top = $(\emptyset, \Sigma^*)$ (dead state, inaccessible state) $r_i = (Pr(q_i), Sc(q_i))$, $i=1,2,3$.

It is easily shown that the transitions in Sat(R) will be the transitions in $\mathcal{A}$ and in addition the useless transitions involving dead and inaccessible state.

So $Sat^-(R_3) = \mathcal{A}_3$. This is quite general: If $\mathcal{A} = Det^-(R) = BDet^-(R)$, then $Sat^-(R) = \mathcal{A}$.

Fig.5.2.1)

EAM	q_1	q_2	q_3
q_1	+	−	−
q_2	−	+	−
q_3	−	−	+

PART II

Properties of Sat(R).

6. The maximal pairs (prime grids) as a lattice L_R.

We define the following partial ordering on K_R:

Definition 6.1

a) $r < r'$ iff $Q(r) \subsetneq Q(r')$

b) $r\downarrow = \{r' | r' \leq r\}$

c) $r\uparrow = \{r' | r' \geq r\}$

By Lemma 4.7.1) $r \leq r'$ <=> $P(r) \supsetneq P(r')$ <=> $(r', e, r) \in M_R$, top = $(R: \Sigma^*, \Sigma^*)$ is the top element, and bottom = $(\Sigma^*, R::\Sigma^*)$ is the bottom element.

Lemma 6.1 If (P_1, Q_1) and (P_2, Q_2) are maximal pairs then

$$P_1 \cap P_2 = \overline{P_1 \cap P_2} \quad \text{and} \quad Q_1 \cap Q_2 = \widetilde{Q_1 \cap Q_2}.$$

Proof:

$$P_1 \cap P_2 = \bar{P}_1 \cap \bar{P}_2 \subseteq \overline{\bar{P}_1 \cap \bar{P}_2} = \overline{P_1 \cap P_2} = \overline{\bar{P}_1 \cap \bar{P}_2} \subseteq \bar{P}_i = \bar{P}_i, \; i=1,2 .$$

Here all inclusions follows by 4.5.2) and all equalities from the fact that $P_i = \bar{P}_i$, i=1,2.

This proves that $Q_1 \cap Q_2$ is the second component in a new maximal pair, which is the greatest lower bound of (P_1, Q_1) and (P_2, Q_2).

Definition 6.2: $(P_1, Q_1) \wedge (P_2, Q_2) = (R:(Q_1 \cap Q_2), Q_1 \cap Q_2)$

$(P_1, Q_1) \vee (P_2, Q_2) = (P_1 \cap P_2, R::(P_1 \cap P_2))$.

This defines the lattice $L_R = (K_R, <)$.

Sat(R) has a large number of transitions and initial/final states (else it would not be saturated). Some simplifications are, however, possible.

Proposition 6.2

1) $r \in S_R \Rightarrow \forall r' \leq r : r' \in S_R$

2) $R \in F_R \Rightarrow \forall r'' \geq r : r' \in F_R$

3) $(r_i, a, r_j) \in M_R \Rightarrow \forall r'' \geq r_i \; \forall r' \leq r_j : (r', a, r'') \in M_R$

Definition 6.3: $Bas(R) = (K_R, \Sigma, M_{Bas}, s_{Bas}, f_{Bas})$ where M_{Bas} contains those transitions $(r_i, a, r_j) \in M_R$ $a \neq e$ which are not implied by other transitions by rule 6.2.3)

$$s_{Bas} = \bigvee_{r \in S_R} r = \left(\bigcap_{e \in P(r)} P(r), R::\bigcap P(r) \right)$$

$$= (\overline{\{e\}}, R::\{e\}) = ([e], R::[e]) = f_1(p_e) \in S_R$$

$$f_{Bas} = \bigwedge_{r \in F_R} r = f_2(q_e) \in F_R.$$

From Bas(R) and the lattice $(K_R, <)$ all of Sat(R) may be reconstructed by rules 6.2.1)2)3).

7. Basic and necessary parts of Sat(R)

We are interested in subautomata $\mathcal{A} \subseteq Sat(R)$, where $T(\mathcal{A}) = R$.

In the search for a minimal NDA for R, all (small) $\mathcal{A} \subseteq Sat(R)$ must be taken into consideration and "$T(\mathcal{A}) = R$?" must be tested.

If some parts of Sat(R) can be proved to belong to all subautomata $\mathcal{A}$ where $T(\mathcal{A}) = R$, this will reduce the search.

<u>Definition 7.1</u>: Given $\mathcal{A} \subseteq Sat(R)$, $\mathcal{A}$ is <u>legitimate</u> iff $T(\mathcal{A}) = R$.

$$Core(R)=\{(r, a, r')\in M_R \mid Sat(R)-(r, a, r') \text{ is not legitimate}\}.$$

Core(R) contains all necessary transitions in Sat(R). In order to give a more explicit way to find Core(R), we first answer the following question: "Given $w\in R$. Which paths in Sat(R) are accepting paths for w?"

Whenever P is an accepting path for w in $\mathcal{A}$, $T(\mathcal{A}) \subseteq R$, there exists an $f:\mathcal{A} \to Sat(R)$ and f(P) will be an accepting path in Sat(R). Especially Det(R) and BDet(R) (via f_1, f_2) induces the two paths $P_D(w)$ and $P_B(w)$.

<u>Definition 7.2</u> Given $w = a^1 \dots a^k \quad a^i\in \Sigma$.
Write $w^i=a^1 \dots a^i$ and $v^i = a^{i+1} \dots a^k$, $i=0,\dots, k$.
Let $P_D(w) = (f_D(e), a^1,\dots,f_D(w^i), a^{i+1},\dots,f_D(w^k))$
where $f_D(u) = f_1(\delta_D(p_e, u)) = ([u], R:[\bar{u}]) = (\bar{u},R:u)$.
Let $P_B(w) = (f_B(w), a^1,\dots,a, f_B(v^i), \dots, f_B(e))$
where $f_B(u) = f_2(\overleftarrow{\delta}_B(q_e,\overleftarrow{u})) = (R::\langle u\rangle, \langle\tilde{u}\rangle) = (R::u, \tilde{u})$

<u>Proposition 7.1</u> Every accepting path for w in Sat(R) lies under $P_D(w)$ and over $P_B(w)$.

<u>More formally</u>: If $(t_0, b_1,\dots, b_\ell, t_\ell)$ $b_i \in \Sigma \cup \{e\}$ $\ell \geq k = |w|$ is an accepting path for w in Sat(R), and we write $t_j = t_j^i$ iff $b_i \dots b_j = w^i$ (iff $b_{j+1} \dots b_\ell = v^i$), then for all $j = 0,\dots,\ell$ (and the corresponding $i\in\{0,\dots,k\}$) the following holds:

$$f_B(v^i) \leq t_j^i \leq f_D(w^i)$$

i.e. (*) $P(t_j^i) \supseteq P(f_D(w^i)) = \overline{[w^i]}$

(**) $Q(f_B(v^i)) = \widetilde{\langle v^i\rangle} \subseteq Q(t_j^i)$

<u>Proof:</u> Since $(t_0, b_1, \dots, b_\ell, t_\ell)$ is an accepting path in $\mathrm{Sat}(R)$ we have the following:

a) $t_0 \in S_R$ or $e \in P(t_0)$

b) $P(t_i)\{b_{i+1}\} \subseteq P(t_{i+1})$ or $\{b_{i+1}\}Q(t_{i+1}) \subseteq Q(t_i)$

c) $t_\ell \in F_R$ or $e \in Q(t_\ell)$

$(*)$ follows from a) and b) by induction on j

$(**)$ follows from b) and c) by induction on $\ell - j$ (or by duality).

<u>Proposition 7.2</u> If $\mathcal{A}$ is a deterministic automaton (without inaccessible states) accepting R, there is a unique homomorphism $f: \mathcal{A} \to \mathrm{Sat}(R)$ determined by $Sc^{\mathcal{A}}(p) = Q(f(p))$.

The corresponding dual statement is also true.

<u>Proof:</u> For $w \in Pr^{\mathcal{C}}(p)$ we have:

$$R::\, Pr^{\mathcal{C}}(p) \subseteq R::\{w\} = w\backslash R$$

And also:

$$u \in w\backslash R \Rightarrow wu \in R = T(\mathcal{A}) = \bigcup_{p' \in Q} Pr^{\mathcal{A}}(p')Sc^{\mathcal{A}}(p') \Rightarrow u \in Sc^{\mathcal{A}}(p)$$

(Since $w \notin Pr(p')$ $p' \neq p$ by determinism). Together with basic properties of the homomorphism $f: \mathcal{A} \to \mathcal{C}$ this gives:

$$w\backslash R \subseteq Sc^{\mathcal{A}}(p) \subseteq Sc^{\mathcal{C}}(f(p)) \subseteq R::Pr^{\mathcal{C}}(f(p)) \subseteq w\backslash R.$$

Which shows $Sc^{\mathcal{A}}(p) = Sc^{\mathcal{C}}(f(p)) = w\backslash R$. When $\mathcal{C} = \mathrm{Sat}(R)$ this gives $Q(f(p)) = Sc^{\mathcal{A}}(p)$.

Especially when $\mathcal{A} = \mathrm{Det}(R)$ $\mathcal{A}$ is reduced and so $p \neq p' \Rightarrow Sc(p) \neq Sc(p')$ which gives $f_1(p) \neq f(p')$ by prop.7.2. i.e., f_1 is injective.

Whenever $\mathcal{A}$ is a DA, $\mathcal{A}^{\wedge} \approx \mathrm{Det}(R)$ and the unique $f: \mathcal{A} \to \mathrm{Sat}(R)$ is given by $f_1 = \phi_1 \circ \phi_2 \circ f_1$ where

$\phi_1 : \mathcal{A} \to \mathcal{A}^{\wedge}$ $\phi_2 : \mathcal{A}^{\wedge} \approx \mathrm{Det}(R)$ $f_1 : \mathrm{Det}(R) \hookrightarrow \mathrm{Sat}(R)$.

Corollary 7.3: $f_1 : \mathrm{Det}(R) \to \mathrm{Sat}(R)$ $f_2 : \mathrm{BDet}(R) \to \mathrm{Sat}(R)$ are the only homomorphisms from Det(R) (BDet(R)) to Sat(R) and they are injective.

Det(R) and $f_1(\mathrm{Det}(R))$ will be used without distinction and it will be convenient to arrange the numbering such that

$$f_1(p_i) = r_i \quad \text{and} \quad f_2(q_i) = r_i \quad \text{for all} \quad r_i \in K_R.$$

Definition 7.3 $K_{Det} = f_1(\hat{P})$ $K_{BDet} = f_2(\hat{Q})$

$$M_{Det} = \{(f_1(p),\ a,\ f_1(\delta_D(p,a))) \mid p \in \hat{P}\ a \in \Sigma\}$$

$$M_{Det} = \{(f_2(\overleftarrow{\delta}_B(q,a)),\ a,\ f_2(q)) \mid q \in \hat{Q}\ \ a \in \Sigma\}$$

$$\mathcal{C} = (K_{\mathcal{C}},\ \Sigma,\ M_{\mathcal{C}})$$

where $M_{\mathcal{C}} = M_{Det} \cap M_{BDet}$ (the common transitions)

$K_{\mathcal{C}} \subseteq K_{Det} \cap K_{Det}$ are the states involved.

Proposition 7.4 Given $(r,\ a,\ r') \in M$. Then $(r,\ a,\ r') \in \mathrm{Core}(R)$, that is there exists $w \in R$ which must use (r, a, r') in order to be accepted in Sat(R).

Proof Choose $w_1 \in Pr^{\mathrm{Det}(R)}(r)$ $w_2 \in Sc^{\mathrm{BDet}}(r')$, and set $w = w_1 a\ w_2$.

By prop. 7.1 all accepting paths P for w lies between $P_D(w)$ and $P_B(w)$. Since these two path coincidence on $(r,\ a,\ r')$, this forces P to use $(r,\ a,\ r')$.

This shows $M_{\mathcal{C}} \subseteq \mathrm{Core}(R)$. In fact we have equality. Put

$$\mathcal{D} = \bigcap_{\text{legitimate } \mathcal{A} \subseteq \mathrm{Sat}(R)} \mathcal{A} = (K_{\mathcal{D}}, \Sigma, M_{\mathcal{D}}, S_{\mathcal{D}}, F_{\mathcal{D}})$$

<u>Proposition 7.5</u>: $M_{\mathcal{C}} = \mathrm{Core}(R) = \bigcap_{\text{legitimate}} \mathcal{A}$.

<u>Proof</u>: It is obvious that $\mathrm{Core}(R) \subseteq M_{\mathcal{D}}$ and that $M_{\mathcal{D}} \subseteq M_{\mathrm{Det}} \cap M_{\mathrm{BDet}} = M_{\mathcal{C}}$.

8. Some properties of the lattice L_R.

In this section we will study the lattice $L_R = (K_R, <)$. We will not be interested in automata and their languages, but mainly in the nodes (points) in K_R and conjunctions/disjunctions over them. It is then easier to regard the nodes as prime grids $(P,Q) \subseteq \hat{P} \times \hat{Q}$ instead of maximal pairs.

The quotients, closures and the imbeddings f_1 and f_2 will then be written as:

$$R::p_i,\ \bar{p}_i,\ R:q_j,\ \tilde{q}_j,\qquad f_1(p_i)=(\bar{p}_i,\ R::p_i)\ \text{etc.}$$

<u>Convention</u> $\bigwedge_{j=1}^{0} = \text{top} \qquad \bigvee_{j=1}^{0} r_j = \text{bottom}.$

For all $A \subseteq K_R$ we will have

$$(\forall r \in A \quad r \leqslant r_0) \Rightarrow \bigwedge_{r\in A} r \leqslant r_0 \qquad \text{even if } A=\emptyset$$

$$(\forall r \in A \quad r \geqslant r_0) \Rightarrow \bigvee_{r\in A} r \geqslant r_0 \qquad \text{even if } A=\emptyset$$

<u>Definition 8.1</u> A node $r \in K_R$ is <u>$\vee$-reducible</u>

$$\text{iff} \quad \exists r, \ldots, r_k: \quad r_j \neq r \qquad r = \bigwedge_{j=1}^{k} r_j \quad k \geq 2$$

$$(\text{iff} \quad \exists\, r_1, \ldots, r_k \quad r_j \lneq r \qquad r = \bigvee_{j=1}^{k} r_j \quad k \geq 2)$$

r is <u>$\wedge$-reducible</u> iff

$$\exists r_1, \ldots, r_k \quad r_j \neq r \quad r = \bigwedge_{j=1}^{k} r_j \quad k \geq 2.$$

<u>Remark:</u> r is $\wedge$-reducible iff r is <u>covered</u> by two or more nodes i.e. there are two or more nodes just over in the lattice-ordering, and similar with $\vee$-reducible.

<u>Definition 8.2:</u> r is <u>$\wedge$-irreducible</u> iff r is covered by exact one node. r is <u>$\vee$-irreducible</u> iff there is exact one node just underneath r in the lattice.

The bottom node may be neither $\vee$-reducible nor $\vee$ irreducible, and similar with the top node. All other nodes, are either reducible or irreducible.

<u>Definition 8.3:</u> $K_R^- = K_R - \{\text{top, bottom}\}$

$D(\wedge\text{-irr}) = \{r \mid r \text{ is } \wedge\text{-irreducible}\}$

$D(\vee\text{-irr}) = \{r \mid r \text{ is } \wedge\text{-irreducible}\}$

$D(\wedge\text{-red}) = \{r \mid r \text{ is } \wedge\text{-reducible}\}$

$D(\vee\text{-red}) = \{r \mid r \text{ is } \vee\text{-reducible}\}$

Then $K_R^- \subseteq D(\wedge\text{-irr}) \cup D(\wedge\text{-red})$

$K_R^- \subseteq D(\vee\text{-irr}) \cup D(\vee\text{-red})$

Definition 8.4: Given $A \subseteq K_R$, $A \neq \emptyset$

$$\bigvee(A) = \{r \mid \exists\ B \subseteq A \quad B \neq \emptyset \quad r = \bigvee_{b \in B} b\}$$

$$\bigwedge(A) = \{r \mid \exists\ B \subseteq A \quad B \neq \emptyset \quad r = \bigwedge_{b \in B} b\}$$

$$\mathrm{VNF}(A) = \bigvee(\bigwedge(A)) \quad \mathrm{KNF}(A) = \bigwedge(\bigvee(A))$$

One may also use $\bigvee^*$ $\bigwedge^*$ VNF^*, KNF^* where $B = \emptyset \subseteq A$ is allowed

Then $\bigvee^*(A) = \bigvee(A) \cup \{\text{bottom}\}$ and

$\bigwedge^*(A) = \bigwedge(A) \cup \{\text{top}\}$.

Lemma 8.1: 1) $D(\wedge\text{-irr}) \subseteq K_{Det}$ 2) $D(\vee\text{-irr}) \subseteq K_{BDet}$

Proof: 1) (2) is by duality): If $r = (P,Q) \in D(\wedge\text{-irr})$, then there is exact one node (P_0, Q_0) covering (P,Q), that is:

$(*)$ $P \supsetneqq P_0$

$(**)$ $((P'Q') \in K_R \wedge P' \subsetneqq P) \Rightarrow P' \subseteq P_0$

We claim: $P = P_0 \cup \{p\}$ $p \notin P_0$. This gives that $P = P_0 \cup \{p\}$ is the least P-component in any prime grid containing p. By 4.6.6) this shows $\bar{p} = P$, so $f_1(p) = (P,Q)$, i.e. $(P,Q) \in K_{Det}$.

Proof of claim: Write $P = P_0 \cup \{p_1, p_2\} \cup A$ where $p_1 \notin P_0$ $p_2 \notin P_0$. Look at $\bar{p}_1$ and $\bar{p}_2$. If $p_i \cap P \subsetneqq P (i=1$ or $i=2)$: then by $(**)$ $p_i \in p_i \cap P \subseteq P_0$ contradicting $p_i \notin P_0$.

So $\bar{p}_1 \supseteq P$ and $\bar{p}_2 \supseteq P$ which gives $p_2 \in \bar{p}_1$ and $p_1 \in \bar{p}_2$ and hence $\bar{p}_1 = \bar{p}_2$. Since $\mathrm{Det}(R)$ is reduced (f_1 is injective) this gives $p_1 = p_2$, showing that $p = P_0 \cup \{p\}$ where $p = p_1 = p_2$.

<u>Lemma 8.2</u>: $D(\wedge\text{-red}) \subseteq \bigwedge(D(\wedge\text{-irr})) \subseteq \bigwedge(K_{Det})$

$D(\vee\text{-red}) \subseteq \bigvee(D(\vee\text{-irr})) \subseteq \bigvee(K_{BDet})$

<u>Proof</u> $D(\wedge\text{-red}) \subseteq \bigwedge(D(\wedge\text{-irr}))$ since the lattice is finite.

<u>Proposition 8.3</u> $K_R^- \subseteq \bigwedge(K_{Det})$, $K_R^- \subseteq \bigvee(K_{BDet})$.

This gives the following easier algorithm in order to generate all prime grids.

<u>Algorithm</u>: Compute $R::p_i = Q_i$ and $R:Q_i = \bar{p}_i$, $p_i \in \hat{P}$. This gives K_{Det}. Take all possible intersections $\cap Q_i$ and compute $R:\cap Q_i$. This gives K_R^-. If top or bottom is lacking compute $(R: \Sigma^*, \Sigma^*)$ and $(\Sigma^*, R::\Sigma^*)$

The following theorem is from Kameda and Weiner [5].

<u>Theorem</u>: If $\mathcal{A} \subseteq \mathrm{Sat}(R)$ is legitimate, then the states must represent prime grids $K_{\mathcal{A}}$ such that all +'entries in RAM(R) must be covered.

<u>Proof</u> For $r \in K_{\mathcal{A}}$ we have

$$T(\mathcal{A}, S, r) \subseteq T(\mathrm{Sat}(R), S, r) = P(r)$$

and $$T(\mathcal{A}, r, F) \subseteq Q(r).$$

If $K_{\mathcal{A}}$ does not cover RAM, there exists a word $w \in R$ where $w \notin P(r)$ $v \notin Q(r)$ for any $r \in K_{\mathcal{A}}$. Then $wv \notin T(\mathcal{A})$.

Lemma 8.4: If $K_{\mathcal{A}}$ covers RAM, then $K_{BDet} \subseteq \bigwedge^{*}(K_{\mathcal{A}})$ and $K_{Det} \subseteq \bigvee^{*}(K_{\mathcal{A}})$.

Proof: If $r_j = (R:q_j, \tilde{q}_j) \in K_{BDet}$, consider

$$T = T(r_j) = \{t \in K \mid r_j \leqslant t\}$$
$$= \{t \in K \mid \tilde{q}_j \subseteq Q(t)\} = \{t \in K \mid q_j \in Q(t)\}$$

Then $r_j \leqslant \bigwedge_{t \in T} t$ is immidiate, and the opposite is equivalent to $R: q_j \subseteq R: \bigcap_{t \in T} Q(t)$ which follows from $K_{\mathcal{A}}$ covering RAM(R).

Proposition 8.5: If $\mathcal{A} \subseteq \mathrm{Sat}(R)$ is legitimate, then $K_R = \mathrm{VNF}^{*}(K_{\mathcal{A}}) = \mathrm{KNF}^{*}(K_{\mathcal{A}})$.

Proof: Write $K_R = \{\text{bottom, top}\} \cup K_R^-$. $\{\text{bottom, top}\} \subseteq \mathrm{KNF}^{*}(K_{\mathcal{A}})$ by convention. $K_R^- \subseteq \mathrm{KNF}^{*}(K_{\mathcal{A}})$ follows by lemma 8.4 and prop. 8.3. The proof for $\mathrm{VNF}^{*}(K_{\mathcal{A}})$ is similar.

9 An example where $(K_R, <) \approx FD(n)$

Throughout this section let $\mathcal{A}$ be an automaton for a language R satisfying:

$$(*) \begin{cases} \mathcal{A} = (S, \Sigma, M, S_0, F) \text{ with } \#S = n \\ \text{and such that the subsetconstruction give} \\ \mathfrak{D}(\mathcal{A}) = (P, \Sigma, M', \{S_0\}, F') \text{ where } P = 2^S \\ \mathfrak{D}(\mathcal{A}^{\leftarrow}) = (Q, \Sigma, M'', \{F\}, F'') \text{ where } Q = 2^S \end{cases}$$

Lemma 9.1: $\mathfrak{D}(\mathcal{A})$ and $\mathfrak{D}(\mathcal{A}^{\leftarrow})$ are both reduced and hence $\mathfrak{D}(\mathcal{A}) \approx \mathrm{Det}(R)$, $\mathfrak{D}(\mathcal{A}^{\leftarrow}) \approx \mathrm{BDet}(R)^{\leftarrow}$, $\hat{P} \approx 2^S$, $\hat{Q} \approx 2^S$.

Proof: It is sufficient to show that $EAM(\mathcal{A})$ is reduced, i.e. different rows (and columns) have different +/- patterns. This is obvious since two rows corresponding to $S_1 \neq S_2$ $S_i \subseteq S$, will disagree on at least one of the coulomns corresponding to $\{s_1\},\ldots,\{s_n\}$.

The (*) property means that every $S' \subseteq S$ represents a state $p = p(S') \in \hat{P}$ in $Det(R)$ and also represents $q = q(S') \in \hat{Q}$ in $BDet(R)$.

Remark: The isomorphism between maximal pairs and prime grids are given by: every state p in $Det(R)$ represents $Pr^{Det}(p) \subseteq \Sigma^*$, and every q in $BDet(R)$ represents $Sc^{BDet(R)}(q) \subseteq \Sigma^*$. Thus one $S' \subseteq S$ will
represent two (possibly different) sets of words over Σ^*. To make this distinction clear we will not write $\hat{P} = 2^S = \hat{Q}$, but use the following isomorphisms: $p: 2^S \to \hat{P}$ $\pi_1: \hat{P} \to 2^S$

$$q: 2^S \to \hat{Q} \quad \pi_2: \hat{Q} \to 2^S$$

We will regard the states in $Sat(R)$ as prime grids, and thus use that version of RAM definition (from [5]), which then reads:

$$RAM(p,q) = 1 \iff \pi_1(p) \cap \pi_2(q) \neq \emptyset$$

Proposition 9.2: L_R is a distributive lattice:

$$(P_i, Q_i) \vee (P_j, Q_j) = (P_i \cap P_j, Q_i \cup Q_j)$$

$$(P_i, Q_i) \wedge (P_j, Q_j) = (P_i \cup P_j, Q_i \cap Q_j)$$

Especially $\widetilde{Q_i \cup Q_j} = Q_i \cup Q_j$ and $\overline{P_i \cup P_j} = P_i \cup P_j$.

Proof (v): It is always true that $R:(P_i \cap P_j) \supseteq Q_i \cup Q_j$. We must show the opposite, which is equivalent to

(1) $\forall q \notin (Q_i \cup Q_j)\colon q \notin R:(P_i \cap P_j)$

and to

(2) $\forall q \notin (Q_i \cup Q_j)\ \exists p \in P_i \cap P_j\ \ \mathrm{RAM}(p,q) = 0.$

Suppose $q \notin Q_i \cup Q_j$. Since $Q_i = R::P_i$ this gives:

$$\exists p' \in P_i\ \mathrm{RAM}(p',q) = 0\ \exists p'' \in P_j\ \mathrm{RAM}(p'',q) = 0$$

Then $\pi_1(p') \cap \pi_2(q) = \emptyset$ and $\pi_1(p'') \cap \pi_1(q) = \emptyset$. Choose $S_0 = \pi_1(p') \cup \pi_1(p'')$ which represents $p_0 = p(S_0) \in \hat{P}$. This p_0 will satisfy the conclusion in (2).

Proposition 9.3: $\bar{p} = \{p^* \in \hat{P} \mid \pi_1(p^*) \supseteq \pi_1(p)\}$

$$\tilde{q} = \{q^* \in \hat{Q} \mid \pi_2(q^*) \supseteq \pi_2(q)\}$$

Proof: Write $\pi_1(p) = \{s_{i_1}, \ldots, s_{i_k}\}$ and $q_{i_j} = q(\{s_{i_j}\})$ (then $\pi_2(q_{i_j}) = \{s_{i_j}\}$). Write $A = \{p^* \in \hat{P} \mid \pi_1(p^*) \supseteq \pi_1(p)\}$.

$$Q = R::p = \{q \mid \mathrm{RAM}(p,q) = 1\} = \{q \mid \pi_2(q) \cap \pi_1(p) \neq \emptyset\}$$

$$= \{q \mid \exists s_{i_j} \in \pi_i(p) : s_{i_j} \in \pi_2(q)\} \supseteq \{q_{i_1}, \ldots, q_{i_k}\}.$$

Thus $\bar{p} = R:Q \subseteq (R:\{q_{i_1}, \ldots, q_{i_k}\}) = \{p^* \in \hat{P} \mid \pi_1(p^*) \cap \pi_2(q_{i_j}) \neq 0,\ \forall j = 1, \ldots, k\}$

$$= \{p^* \in \hat{P} \mid \{s_{i_1}, \ldots, s_{i_k}\} \subseteq \pi_1(p^*)\} = A.$$

For the opposite: If $p^* \in A$, then for all $q \in Q = R:p$ we have

$$\pi_1(p^*) \supseteq \pi_1(p) \quad \text{and} \quad \pi_2(q) \cap \pi_1(p) \neq \emptyset,$$

and hence $\pi_1(p) \cap \pi_2(q) \neq \emptyset$, showing $p^* \in R:Q = \bar{p}$.

<u>Proposition 9.4</u>: For all $P \subseteq \hat{P}$, $Q \subseteq \hat{Q}$:

$$\bar{P} = \{p^{\star} \in \hat{p} \mid \exists p \in P: \pi_1(p^{\star}) \supseteq \pi_1(p)\}$$

$$\tilde{Q} = \{q^{\star} \in \hat{Q} \mid \exists q \in Q: \pi_2(q^{\star}) \supseteq \pi_2(q)\}$$

<u>Proof</u>: By 9.3 and 9.2 and general properties of :, ::, - and ~.

This relates closely to te term J-closed from Birkhoff "Lattice theory" [1]:

Given $X = \{x_1, \ldots, x_n\}$ $I = \{1, \ldots, n\}$. Let σ, τ denote subsets of I. Let H,F denote subsets of 2^I.

H is J-closed iff $\sigma \in G \Rightarrow \forall \sigma^{\star} \supseteq \sigma: \sigma^{\star} \in H$. When $H^{\star}$ denotes the J-closure we have:

$$H^{\star} = \{\sigma^{\star} \mid \exists \sigma \in H \ \sigma^{\star} \supseteq \sigma\}.$$

The relation to prop. 9.4 is immidiate.

Every element in FD(n) (<u>the free distributive lattice</u> generated by $X = \{x_1, \ldots, x_n\}$) can be written in conjunctive normal form

$$\bigvee_{\sigma \in H} \bigwedge_{i \in \sigma} x_i = \bigvee_{\sigma \in H^{\star}} \bigwedge_{i \in \sigma} x_i$$

<u>Theorem</u>: FD(n) $\approx$ the ring at all J-closed sets $H^{\star} \subseteq 2^X$.

<u>Ex. (n=3)</u>: If $H = \{\{1,2\}, \{1,3\}\}$. Then $H^{\star} = \{\{1,2\}, \{1,3\}, \{1,2,3\}\}$ and $(x_1 \wedge x_2) \vee (x_1 \wedge x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$.
We are now prepared for the definition of the isomorphism between FD(n) and $(K_R, <)$, $\phi: \{H \subseteq 2^X \mid H = H^{\star}\} \to K_R$.

Definition 9.1 Given $\sigma \subseteq I$ write

$$s(\sigma) = \{s_i | i \in \sigma\} \subseteq S$$

$$q(\sigma) = q(s(\sigma)) \in \hat{Q}$$

$$q(H) = \{q(\sigma) | \sigma \in H\} \subseteq \hat{Q}$$

Define $\phi(H^*) = (R:q(H^*), q(H^*))$.

Since H^* is closed, also $g(H^*)$ is closed by prop. 9.4, and thus $q(H^*) = \widetilde{q(H^*)}$ and $\phi(H^*)$ is an element of K_R.

Lemma 9.5:

1) $q(H_1^* \cap H_2^*) = q(H_1^*) \cap q(H_2^*)$ 2) $q(H_1^* \cup H_2^*) = q(H_1^*) \cup q(H_2^*)$

3) $H_1^* \subsetneqq H_2^* \Rightarrow q(H_1^*) \subsetneqq q(H_2^*)$ 4) $H_1^* \neq H_2^* \Rightarrow q(H_1^*) \neq q(H_2^*)$

5) $\phi(H_1^* \wedge H_2^*) = \phi(H_1^*) \wedge \phi(H_2^*)$ 6) $\phi(H_1^* \vee H_2^*) = \phi(H_1^*) \vee \phi(H_2^*)$

Proof: 1)-4) are immediate, 5)-6) follows from 1)-4) and prop. 9.2.

Definition 9.2 Write $p_i = p(\{s_i\})$, $q_i = q(\{s_i\})$.

Let $r_i = f_1(p_i) = (\bar{p}_i, R::p_i) =$

$$= (\{p^* \in \hat{P} | s_i \in \pi_1(p^*)\}, \{q^* \in \hat{Q} | s_i \in \pi_2(q^*)\}) = (R:q_i, \tilde{q}_i) = f_2(q_i)$$

Lemma 9.6: $q(\{i\}^*) = \tilde{q}_i$ and ϕ is surjective.

Proof:

$$q(\{i\}^*) = \{q(\sigma) | \sigma \in \{i\}^*\} = \{q(s(\sigma)) | i \in \sigma \subseteq I\}$$

$$= \{q(S') | s_i \in S' \subseteq S\} = \{q(\pi_2(q^*)) | s_i \in \pi_2(q^*)\} = \{q^* | s_i \in \pi_2(q^*)\} = \tilde{q}_i.$$

Thus $\phi(\{i\}^*) = r_i = (R:q_i, \tilde{q}_i)$ $i=1,\dots,n$ and ϕ is onto $\{r_1,\dots,r_n\}$ $\{r_1,\dots,r_n\}$ covers RAM(R), and by lemma 8.4 and prop.8.5. $\{r,\dots,r_n\}$ generates K_R, and hence ϕ is onto K_R.

<u>Proposition 9.7:</u> $L_R = (K_R,<) \approx FD(n)$

<u>Proof;</u> By 9.5 and 9.6 it follows that ϕ is an isomorphism.

<u>Ex.9.1.</u> (S. Aanderaa) There are lots of automta and languages R satisfying the condition (*) studied in this section. (E.g. given n, let $\Sigma=\{1,2,\dots,2^n\}$). The interesting thing is that FD(n) can be achieved using only a 4-letter alphabet $\Sigma=\{0,1,2,3\}$.

Consider the following automata $\mathcal{A}(3), \mathcal{A}(4), \dots$ shown in fig. 9.1).

Let $R(n) = T(\mathcal{A}(n))$. Here $R(n) = R(n)^T$ and $\mathcal{A}(n) \approx \mathcal{A}(n)^{\leftarrow}$, so $\mathfrak{D}(\mathcal{A}(n)) \approx \mathfrak{D}((\mathcal{A}(n))^{\leftarrow})$, and in order to show that $\mathcal{A}(n)$ satisfies (*) it is enough to show that $\mathfrak{D}(\mathcal{A}(n))$ has 2^n states.

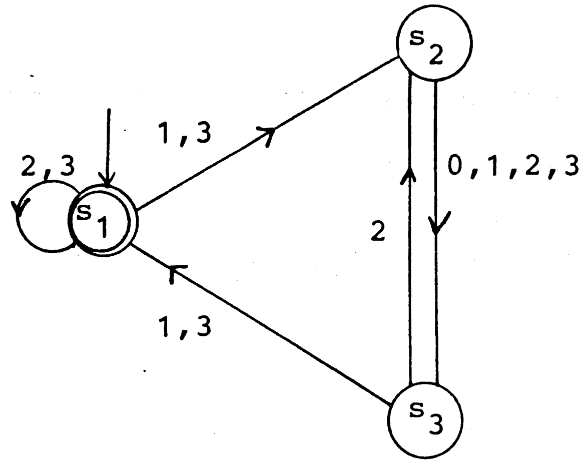
Prop. 9.7 then gives $(K_{R(n)},<) \approx FD(n)$.

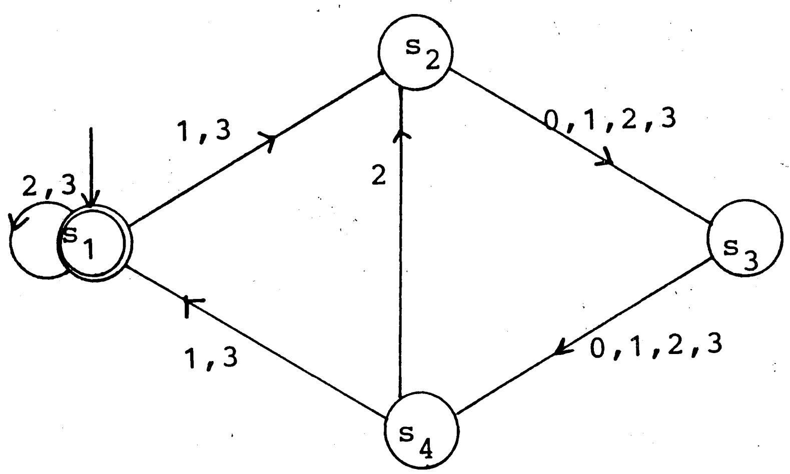
<u>Claim:</u> $\mathfrak{D}(\mathcal{A}(n))$ has 2^n states.

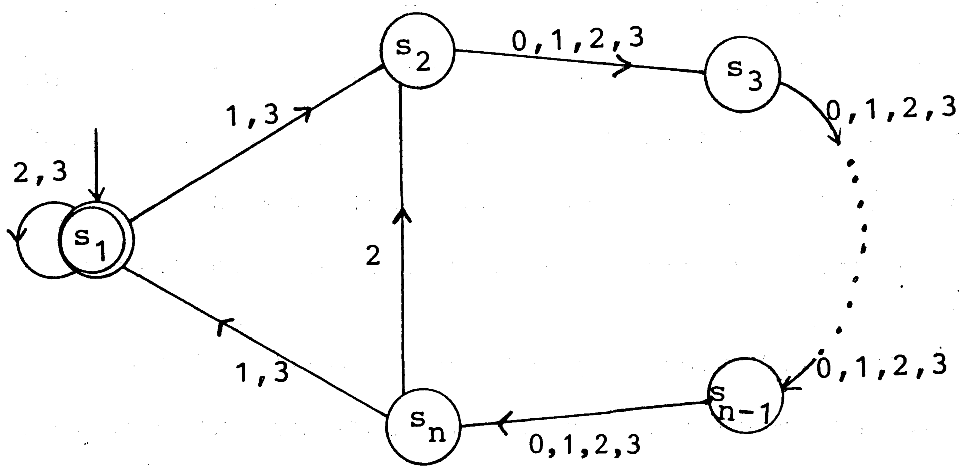
<u>Proof:</u> We see that 1 represents cyclic rotation and that 21^{n-1} represents change of 2 elements. $(s_1,s_2,\dots,s_n)$ is via 1 changed to $(M(s_1,1), M(s_2,1),\dots,M(s_n,1)) = (s_2,s_3,\dots,s_1)$

And $(s_n, s_1, s_2,\dots,s_{n-1})$ is via 2 changed to
$(s_2, s_1, s_3,\dots,s_n)$ which via 1^{n-1} is changed to
$(s_1,s_n, s_2,\dots,s_{n-1})$

Fig.9.1)


s 2
1,3
2,3
0,1,2,3
s 1
2
1,3
s 3


s 2
1,3
0,1,2,3
2
2,3
s 1
s 3
1,3
0,1,2,3
s 4


s 2
0,1,2,3
s 3
1,3
0,1,2,3
2,3
s 1
2
1,3
0,1,2,3
s n
s n-1
0,1,2,3

These two permutations generates all permutations of $\{s,\ldots,s_n\}$. So it is enough to show that the states

$\emptyset$, $\{s_1\}$, $\{s_1,s_2\}$, $\{s_1,\ldots,s_j\}$, ..., $\{s_1,\ldots,s_n\}$ are in ((n)).

But that is obvious, since

$$M(s_1,0) = \emptyset \quad M(s_1,2) = \{s\},\ M(s_1,3) = \{s_1,s_2\} \quad \text{and}$$

$$M(\{s_1,\ldots,s_{j-1}\},3) = \{s_1,\ldots,s_j\} \quad \text{when} \quad 2 \leqslant j \leqslant n.$$

10 Further work

In this paper we have studied, for a given event R, Sat(R), the lattice L_R and accepting paths for $w \in R$ in Sat(R).

By duality we know that $\mathrm{Sat}(R^T) \approx \overleftarrow{\mathrm{Sat}(R)}$. We have <u>not</u> studied how Sat(R) and $\mathrm{Sat}(R^C)$ relates.

It would also be interesting to know e.g. the relations between Sat(R) and Sat(w\R) and between $\mathrm{Sat}(R_1)$ and $\mathrm{Sat}(R_1 \cdot R_2)$.

Acknowledgements

This paper is based on my cand.scient thesis (in Norwegian) at the University of Oslo. I want to thank my advisor Professor Stål Aanderaa for his guidance and for a number of good ideas and examples. The idea of a minimal saturated automaton and the construction of Sat(R) given in section 4, are both entirely due to him.

Thanks also to Herman Ruge Jervell and Jens Erik Fenstad for useful comments on earlier versions of the manuscript.

REFERENCES

[1] Birkhoff G.: "Lattice Theory"
American Math. Society Colloquium Publ.
Vol. XXV. 1961.

[2] Cohen R.S., Brzozowski J.: "General properties of star height of regular events",
J. Comput. System Sci. 4(1970) pp. 260-280.

[3] Eggan, L.C: "Transition graphs and the star height of regular events"
Michigan Math. J. 10(1963) pp. 385-397.

[4] Hopcroft J.E., Ullmann J.D: "Introduction to automta theory, languages and computation"
Addison-Wesley Publ.Comp. 1979.

[5] Kameda T., Weiner P.: "On the state minimazation of non-deterministic finite automata". IEEE Transactions on Computers. Vol. C-19 No.7 July 1970 pp. 617-627.

[6] Kristiansen L: "Saturated automata applied to the star height problem".
Preprint Series 3 (1986) University of Oslo.

[7] McNaughton R: "An introduction to regular expressions"
Applied Automata Theory 1968 pp.35-54.